UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/834,106	04/13/2001	Bao Feng	45539-20009.00	5315

25227 7590 10/18/2005

MORRISON & FOERSTER LLP
1650 TYSONS BOULEVARD
SUITE 300
MCLEAN, VA 22102

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/834,106	FENG ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) *1-8* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on August 24, 2005. Claims 1 – 8 are cancelled and new Claims 9 – 32 have been added. Therefore, Claims 9 – 32 are pending.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Singapore on 04/13/2000. It is noted, however, that applicant has not filed a certified copy of the 200002034-7 application as required by 35 U.S.C. 119(b).

Claim Objections

3. Claims 12, 16, 20, 24, 28 and 21 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 9 – 12, 17 – 19, 25 – 28 and 32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent and new Claims 9, 17 and 25 read, "...encrypting the plurality of encryption keys using a first key...".

With respect to "...encrypting the plurality of encryption keys using a first key...", although the specification discloses "Finally, the database 104 encrypts the keys themselves to obtain $s_i = k_i^R \bmod p$, i=1,2,...N 208.", the specification does not disclose a method for "...encrypting the plurality of encryption keys using a first key...". The specification does not indicate how "...a first key..." is generated, retrieved or accessed to encrypt the plurality of encryption keys to generate a plurality of encryption key ciphertexts. Applicant amendment does not clarify the steps of "...encrypting the plurality of encryption keys using a first key...".

The dependent claims 10 – 12, 18 – 20, 26 – 28 and 32 are rejected at least by virtue of their dependency on the dependent claims.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 9 – 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

The examiner will interpret the claims as best understood for applying the appropriate art for rejection purposes.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 9 – 32 are rejected under 35 U.S.C. 102(b) as being anticipated by Gammie (U.S. Patent Number 5,029,207).

7. Regarding Claims 9, 17 and 25 Gammie

discloses generating a plurality of encryption keys associated with a plurality of digital objects stored in an electronic database (Summary and Column 9 line 65 – Column 10 line 13);

encrypting the plurality of digital objects using the plurality of associated encryption keys to generate a plurality of digital object ciphertexts (Summary and Column 9 line 65 – Column 10 line 15);

encrypting the plurality of encryption keys using a first key to generate a plurality of encryption key ciphertexts (Summary and Column 9 line 65 – Column 10 line 15);

transmitting to a requester the digital object ciphertexts and encryption key ciphertexts (Summary and Column 9 line 65 – Column 10 line 13);

receiving from the requester an encryption key ciphertext further encrypted using a second key (Summary and Column 9 line 65 – Column 10 line 20);

decrypting the received encryption key ciphertext using the first key to generate a partially decrypted encryption key (Summary and Column 9 line 65 – Column 10 line 29); and

transmitting the partially decrypted encryption key to the requester (Summary and Column 9 line 65 – Column 10 line 37).

8. Regarding Claims 13, 21 and 29 Gammie discloses requesting a plurality of digital objects from an electronic database (Summary and Column 12 lines 21 – 36);

receiving from the database a plurality of ciphertext digital objects (Summary and Column 12 lines 21 – 36);

receiving from the database a plurality of ciphertext keys associated with the plurality of ciphertext digital objects (Summary and Column 12 lines 21 – 36);

selecting a ciphertext key from the plurality of ciphertext keys (Summary and Column 12 lines 21 – 36);

further encrypting the selected ciphertext key using a first key to generate a further encrypted ciphertext key (Summary and Column 12 lines 21 – 36);

transmitting the further encrypted ciphertext key to the database (Summary and Column 12 lines 21 – 36);

receiving from the database a ciphertext key partially decrypted using a second key (Summary and Column 12 lines 21 – 36);

decrypting the partially decrypted ciphertext key using the first key to generate a decrypted key (Summary and Column 12 lines 21 – 36); and

decrypting the received ciphertext digital object using the decrypted key (Summary and Column 12 lines 21 – 36).

9. Claims 10, 14, 18, 22, 26 and 30 are rejected as applied above in rejecting Claims 9, 13, 17, 21, 25 and 29. Furthermore, Gammie teaches encrypting the plurality

of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key (Column 2 lines 14 – 28).

10. Claims 11, 15, 19, 23, 27 and 31 are rejected as applied above in rejecting Claims 9, 13, 17, 21, 25 and 29. Furthermore, Gammie teaches decrypting the received encryption key ciphertext by determining (encryption key ciphertext)$^{(1/(\text{random number R}) \text{ mod } (\text{prime number p-1}))}$ mod (prime number p) (Column 2 lines 14 – 28).

11. Claims 12, 16, 20, 24, 28 and 32 are rejected as applied above in rejecting Claims 10, 14, 18, 22, 26 and 27. Furthermore, Gammie teaches performing the modulo operation if computation of a discrete logarithm is infeasible (Column 2 lines 14 – 28).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

14. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
October 12, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100